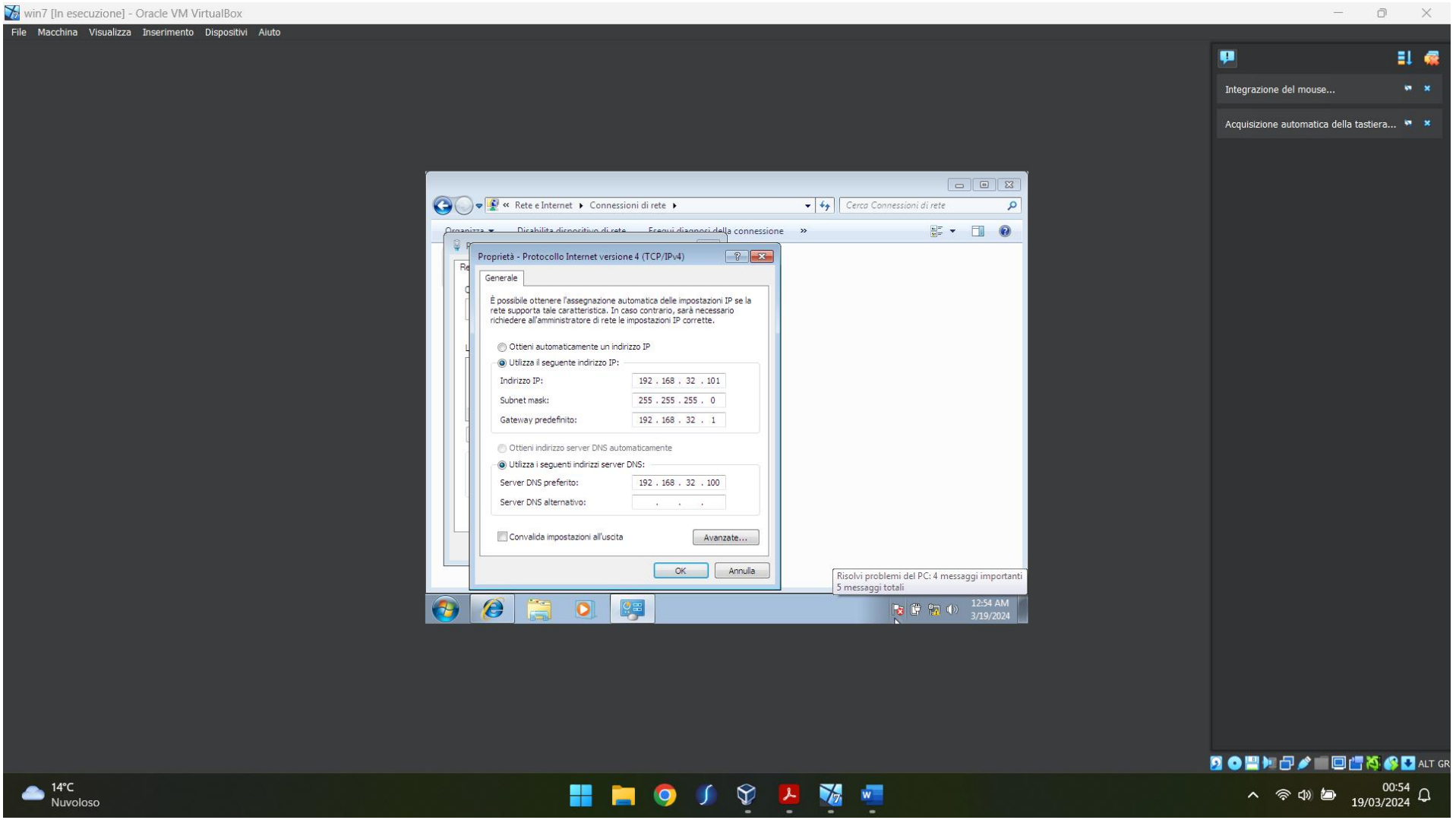
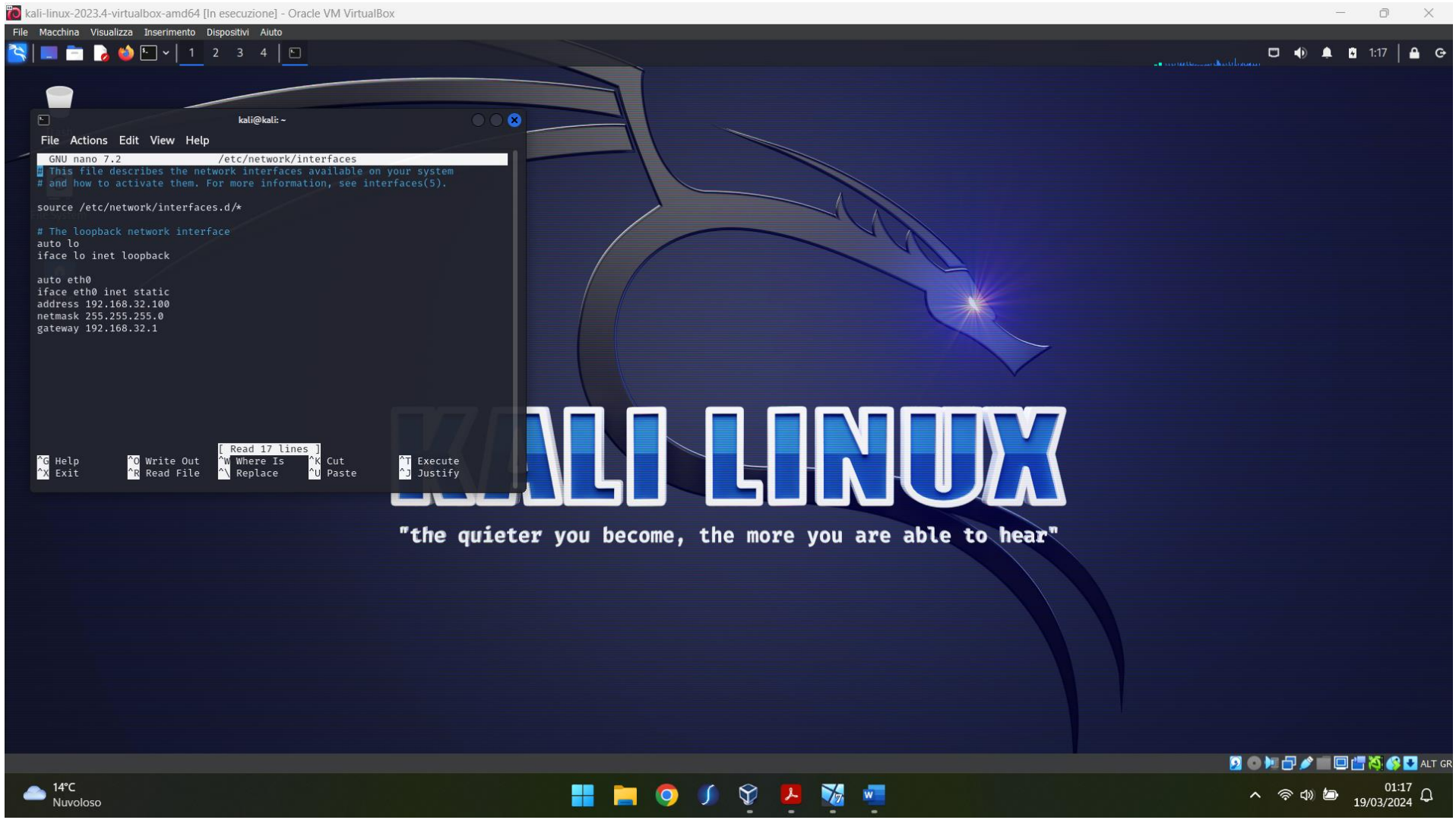
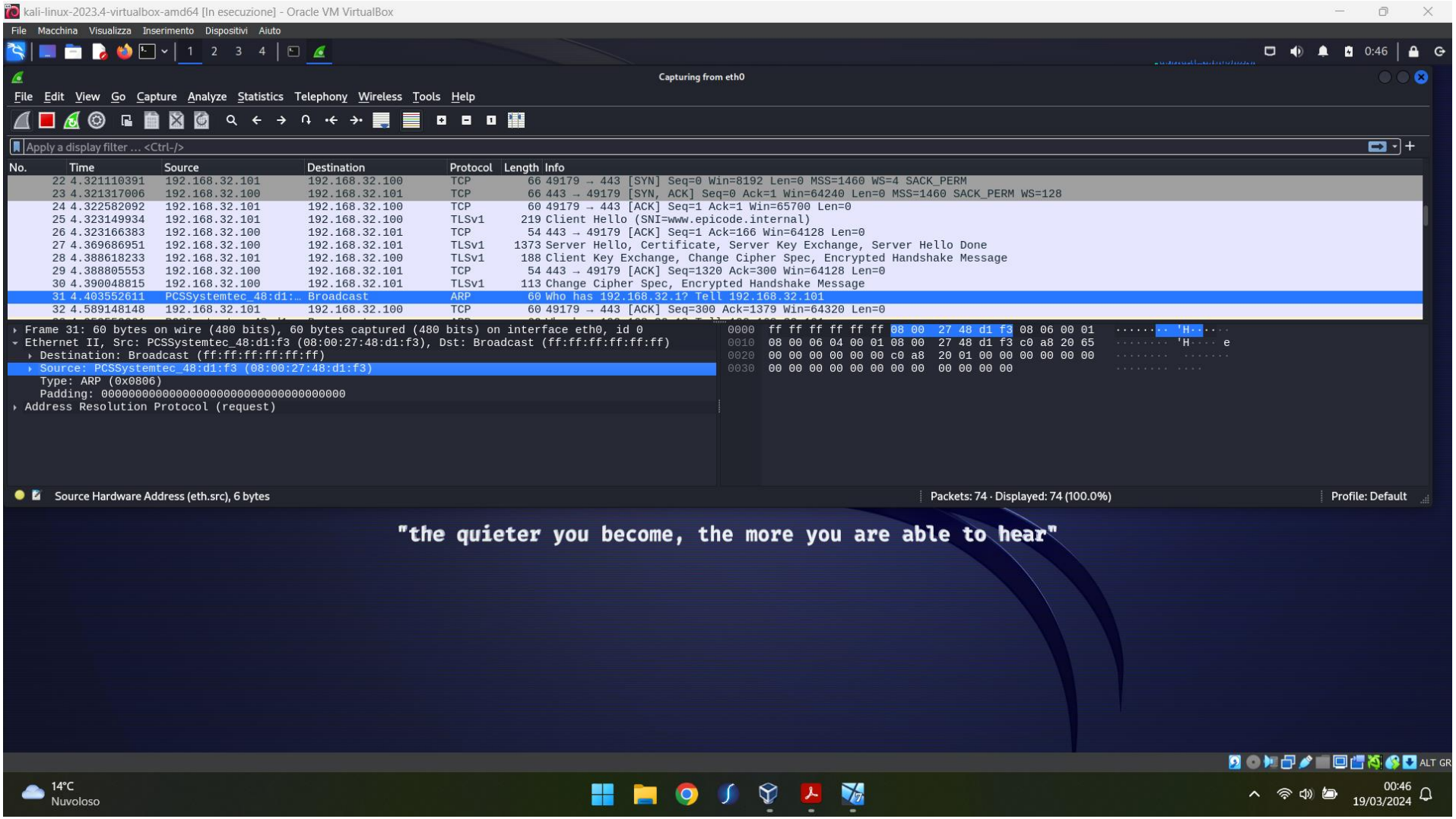
Configurazione IP e DNS server su terminale Window7 con IP 192.168.32.101, gateway predefinito 192.162.32.1 e DNS 192.168.32.100 (IP Kali)



Configurazione IP Kali 192.168.32.100 con comando sudo nano /etc/network/interfaces

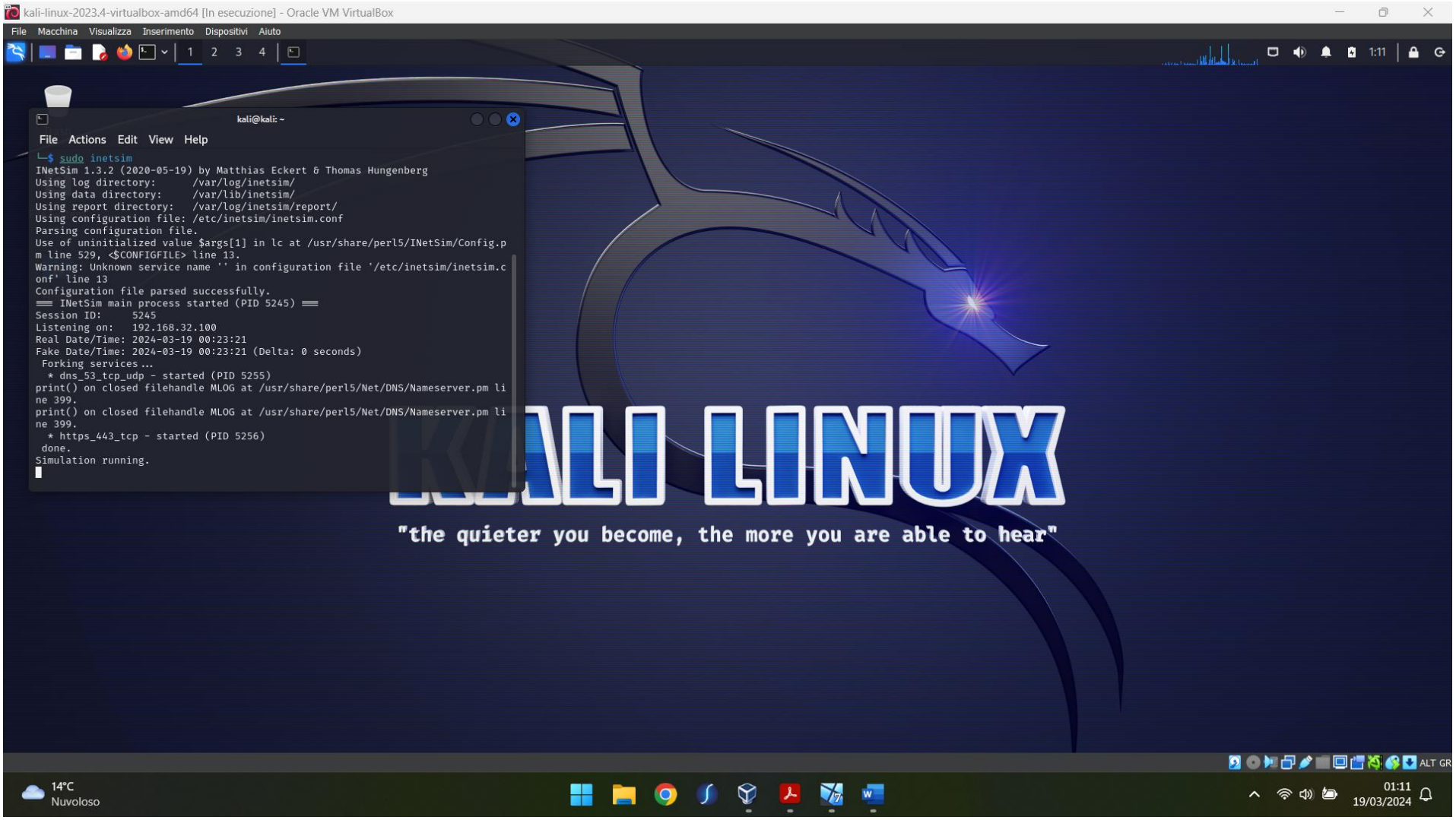


CATTURA WIRESHARK HTTPS – TCP WINDOWS 7 E KALI

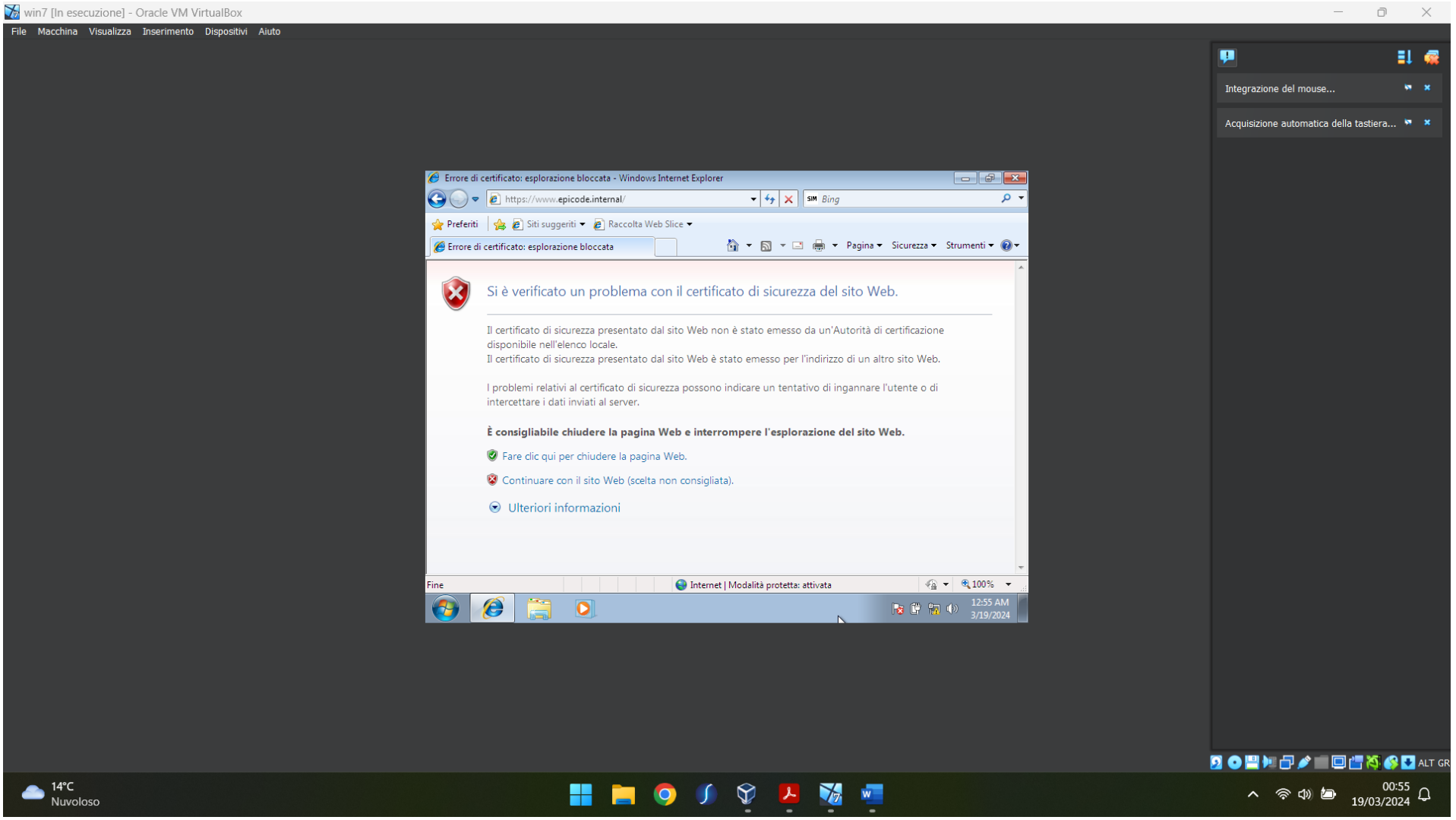


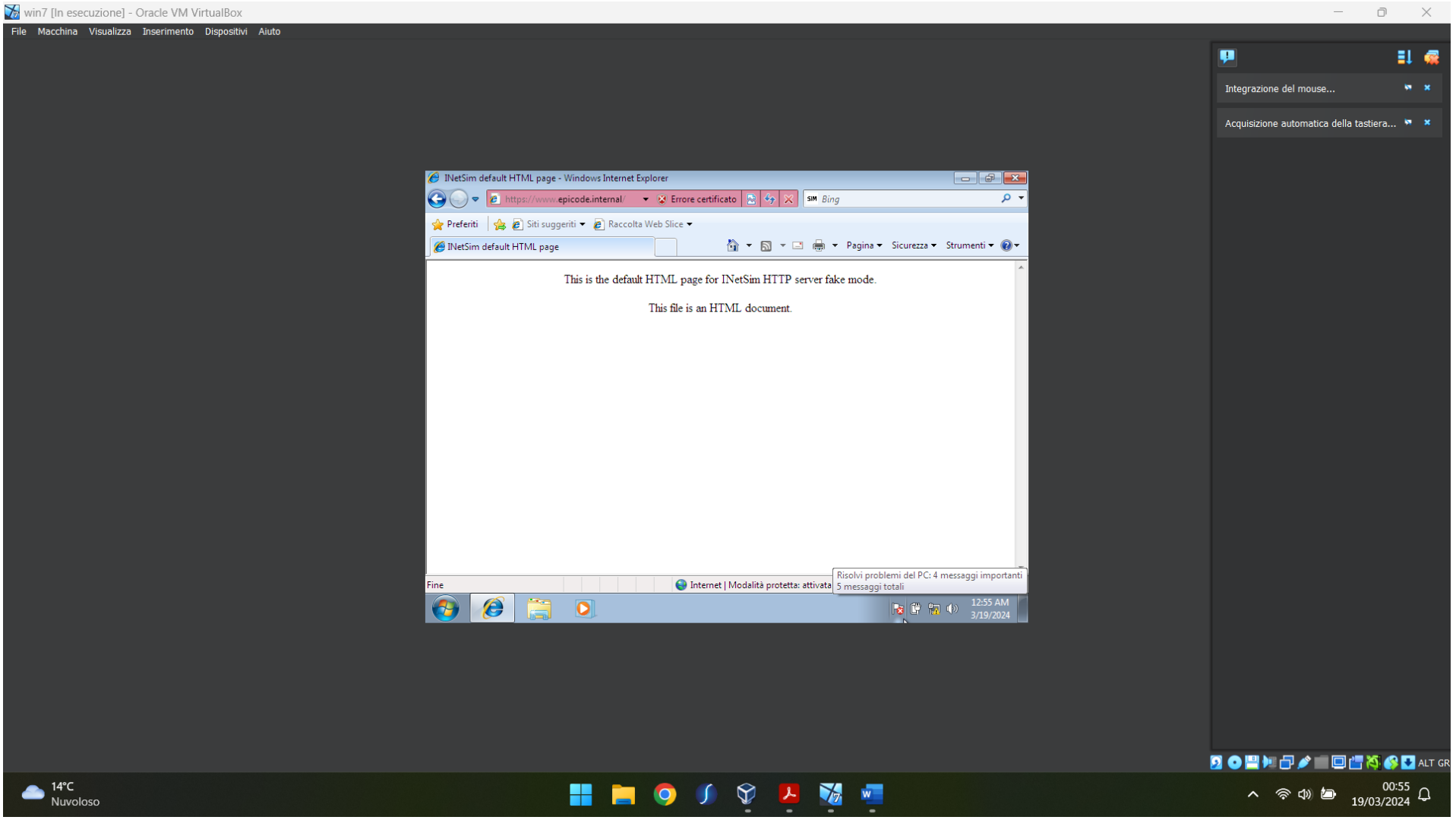
SOURCE MAC KALI 08:00:27:21:b1:d0 – MAC DESTINATION WIN7 08:00:27:48:d1:f3

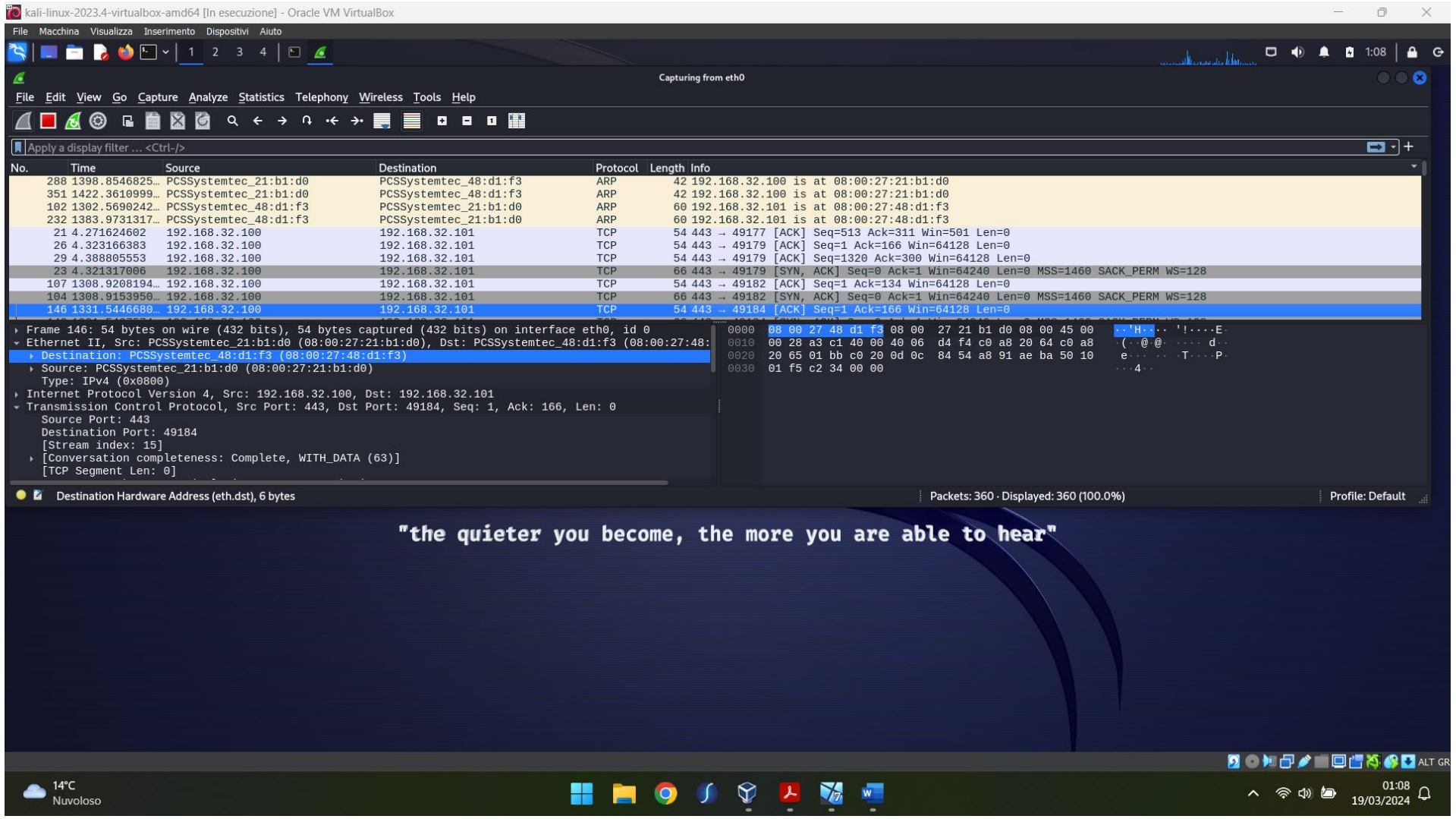
Attivazione inetsim


kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
1:11
kali@kali: ~
File Actions Edit View Help
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Use of uninitialized value $args[1] in lc at /usr/share/perl5/INetSim/Config.pm line 529, <$CONFIGFILE> line 13.
Warning: Unknown service name '' in configuration file '/etc/inetsim/inetsim.conf' line 13
Configuration file parsed successfully.
=== INetSim main process started (PID 5245) ===
Session ID: 5245
Listening on: 192.168.32.100
Real Date/Time: 2024-03-19 00:23:21
Fake Date/Time: 2024-03-19 00:23:21 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 5255)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* https_443_tcp - started (PID 5256)
done.
Simulation running.
KALI LINUX
"the quieter you become, the more you are able to hear"
ALT GR
14°C
Nuvoloso
01:11
19/03/2024

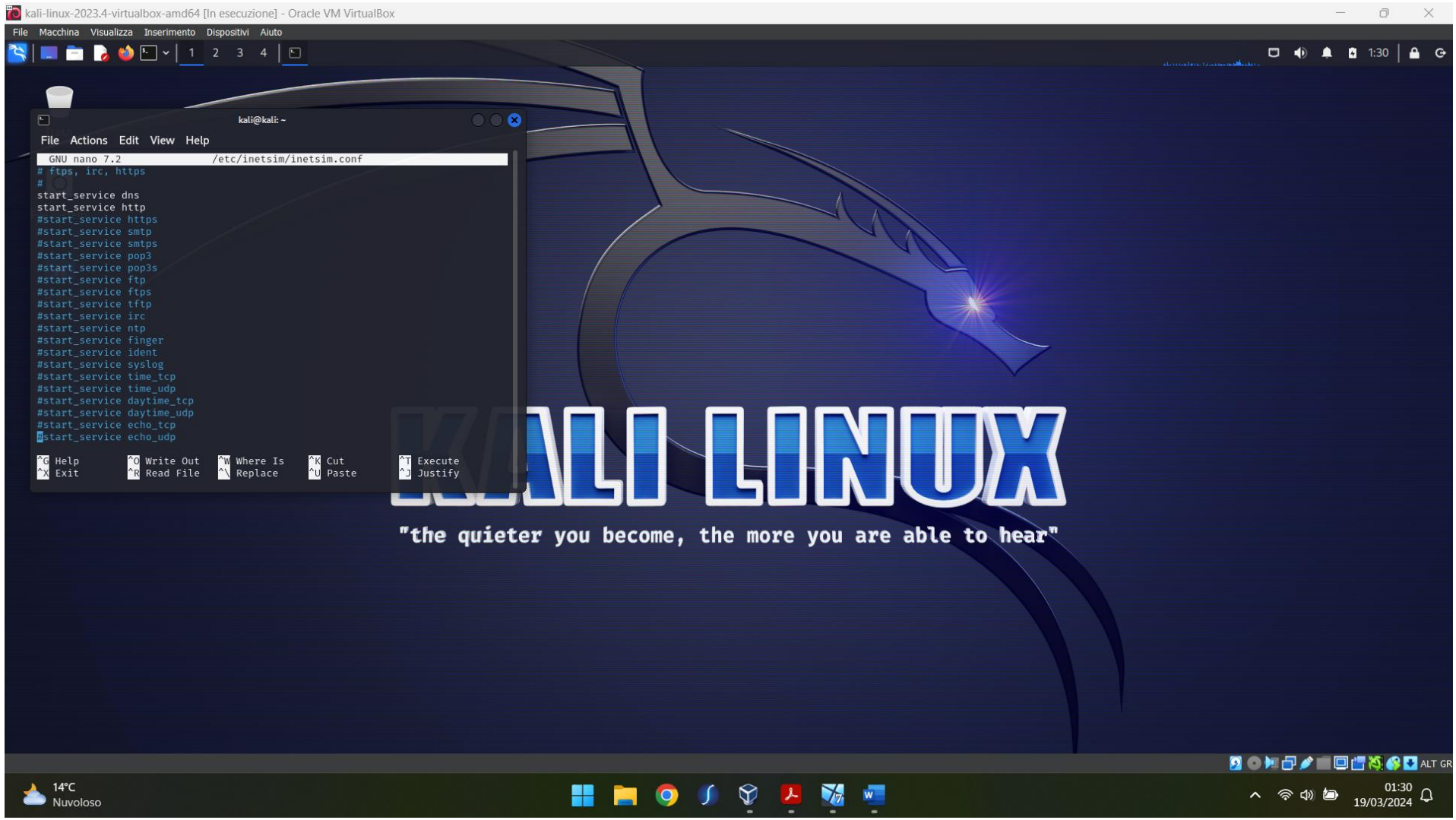
Richiesta da client window7



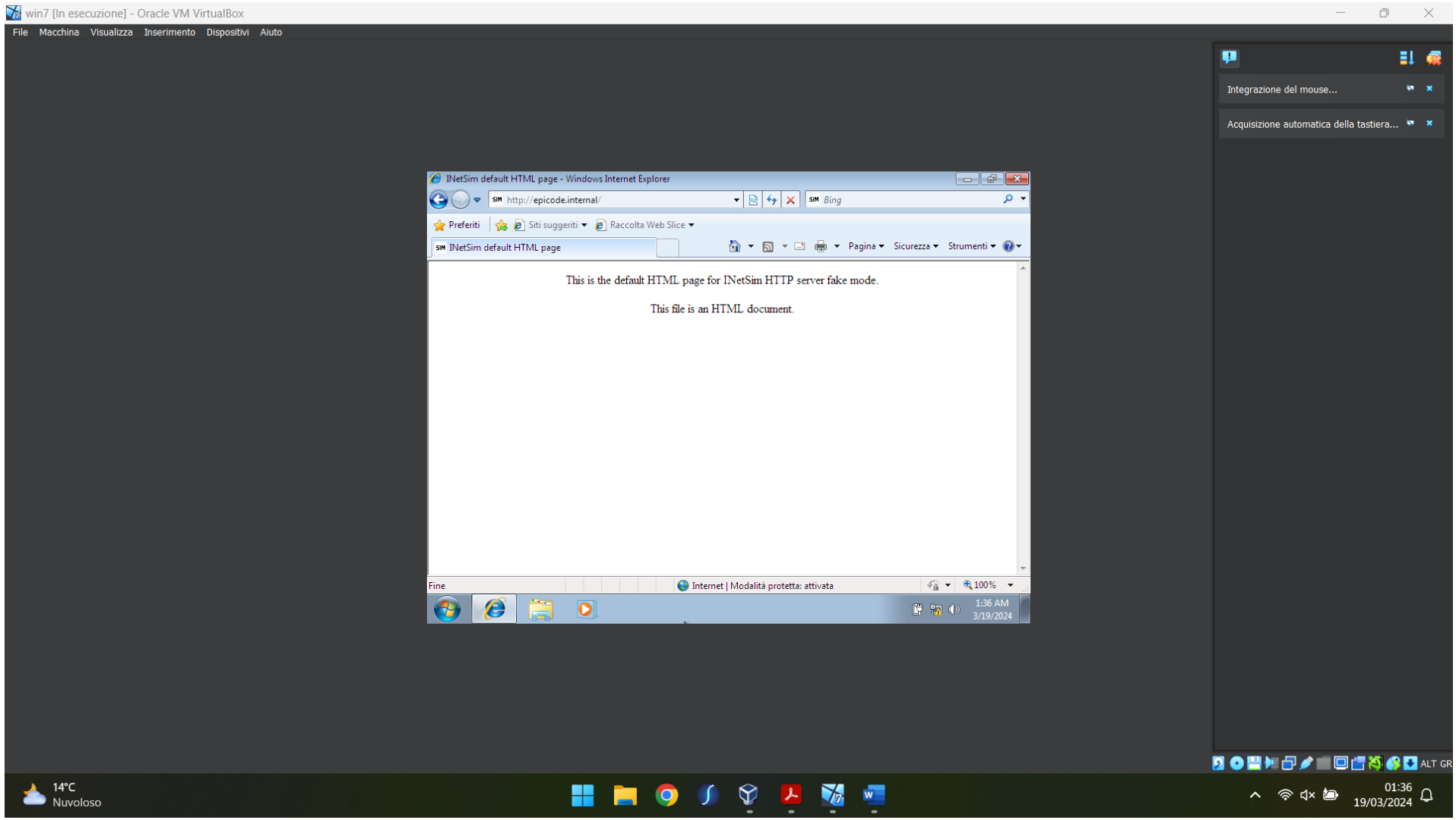

win7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Integrazione del mouse...
Acquisizione automatica della tastiera...
INetSim default HTML page - Windows Internet Explorer
https://www.epicode.internal/
Errore certificato
Bing
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
Pagina
Sicurezza
Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
Risolvi problemi del PC: 4 messaggi importanti
5 messaggi totali
12:55 AM
3/19/2024
ALT GR
14°C
Nuvoloso
00:55
19/03/2024


kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
288 1398.8546825… PCSSystemtec_21:b1:d0 PCSSystemtec_48:d1:f3 ARP 42 192.168.32.100 is at 08:00:27:21:b1:d0
351 1422.3610999… PCSSystemtec_21:b1:d0 PCSSystemtec_48:d1:f3 ARP 42 192.168.32.100 is at 08:00:27:21:b1:d0
102 1302.5690242… PCSSystemtec_48:d1:f3 PCSSystemtec_21:b1:d0 ARP 60 192.168.32.101 is at 08:00:27:48:d1:f3
232 1383.9731317… PCSSystemtec_48:d1:f3 PCSSystemtec_21:b1:d0 ARP 60 192.168.32.101 is at 08:00:27:48:d1:f3
21 4.271624602 192.168.32.100 192.168.32.101 TCP 54 443 → 49177 [ACK] Seq=513 Ack=311 Win=501 Len=0
26 4.323166383 192.168.32.100 192.168.32.101 TCP 54 443 → 49179 [ACK] Seq=1 Ack=166 Win=64128 Len=0
29 4.388805553 192.168.32.100 192.168.32.101 TCP 54 443 → 49179 [ACK] Seq=1320 Ack=300 Win=64128 Len=0
23 4.321317006 192.168.32.100 192.168.32.101 TCP 66 443 → 49179 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
107 1308.9208194… 192.168.32.100 192.168.32.101 TCP 54 443 → 49182 [ACK] Seq=1 Ack=134 Win=64128 Len=0
104 1308.9153950… 192.168.32.100 192.168.32.101 TCP 66 443 → 49182 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
146 1331.5446680… 192.168.32.100 192.168.32.101 TCP 54 443 → 49184 [ACK] Seq=1 Ack=166 Win=64128 Len=0
Frame 146: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_21:b1:d0 (08:00:27:21:b1:d0), Dst: PCSSystemtec_48:d1:f3 (08:00:27:48:
Destination: PCSSystemtec_48:d1:f3 (08:00:27:48:d1:f3)
Source: PCSSystemtec_21:b1:d0 (08:00:27:21:b1:d0)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 443, Dst Port: 49184, Seq: 1, Ack: 166, Len: 0
Source Port: 443
Destination Port: 49184
[Stream index: 15]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
0000 08 00 27 48 d1 f3 08 00 27 21 b1 d0 08 00 45 00
0010 00 28 a3 c1 40 00 40 06 d4 f4 c0 a8 20 64 c0 a8
0020 20 65 01 bb c0 20 0d 0c 84 54 a8 91 ae ba 50 10
0030 01 f5 c2 34 00 00
Destination Hardware Address (eth.dst), 6 bytes
Packets: 360 · Displayed: 360 (100.0%)
Profile: Default
"the quieter you become, the more you are able to hear"
14°C
Nuvoloso
01:08
19/03/2024

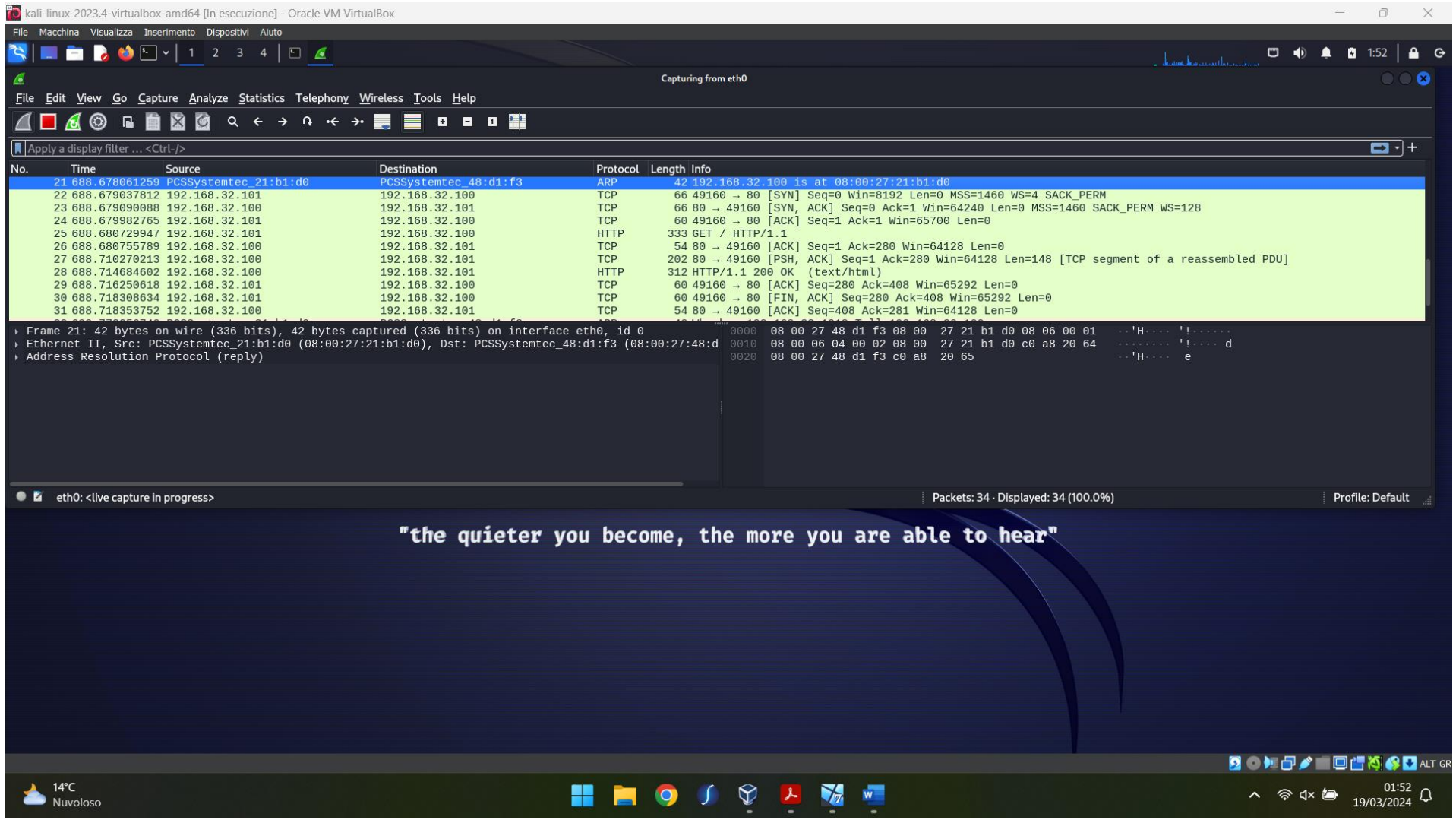
Si ripete stessa procedura questa volta su http



PUNTAMENTO SU WIN7 http EPICODE.INTERNAL



CATTURA CON WIRESHARK http



CONCLUSIONE

SESSIONI TCP IN http NON SONO SICURE PERCHE’ IN CHIARO A DIFFERENZA DI QUELLE HTTPS CHE SONO CIFRATE GRAZIE CRITTOGRAFIA TLS